Цели атаки:

- Бумажный мусор в мусорных корзинах, расположенных вне организации
- Бумажный мусор в мусорных корзинах, расположенных внутри организации
- Выброшенные электронные носители

Описание:

- Изучая документы, извлеченные из внешних мусорных контейнеров, злоумышленник узнает важную корпоративную информацию.
- Обходя принятые в организации принципы управления внешним мусором, злоумышленник ворует документы из мусорных корзин, расположенных в самой организации.
- Злоумышленник ворует данные и приложения, хранящиеся на выброшенных электронных носителях, и сами носители.

Ущерб

- **Утечка конфиденциальной информации**
- Урон репутации компании
- Трата ресурсов

Сотрудники компании должны понимать все последствия, к которым может привести выбрасывание бумажных документов или электронных носителей информации в мусорную корзину. Как только мусор покидает территорию компании, ее права могут больше на него не распространяться.
Бумажный мусор всегда следует измельчать в бумагорезательных машинах, а электронный — уничтожать или стирать записанные на нем данные. Если какие-либо документы (например телефонный справочник) из-за размеров или жесткости невозможно измельчить в бумагорезательной машине либо у пользователя нет технической возможности это сделать, нужно определить специальную процедуру избавления от них. Мусорные контейнеры следует размещать в защищенной области, недоступной посторонним лицам.

При разработке политики утилизации мусора важно убедиться в том, что соблюдены все местные санитарные нормы и нормы безопасности. По мере возможности следует выбирать экологически чистые способы утилизации мусора.

Кроме внешнего мусора — бумажных или электронных отходов, доступных посторонним

лицам, — есть еще и внутренний, который тоже нужно контролировать. При определении политик безопасности это часто упускают из виду, предполагая, что любому, кто имеет доступ на объекты компании, можно доверять. Ясно, что это не всегда так. Одной из самых эффективных мер по управлению бумажным мусором является классификация данных. Для этого следует определить разные категории бумажных документов и способы их утилизации. Ниже перечислены примеры таких категорий.

- Конфиденциальная
- корпоративная информация.

Прежде чем выбросить какие-либо документы с конфиденциальной корпоративной информацией в мусорный контейнер , их необходимо измельчить в бумагорезательной машине.
Закрытая информация. Прежде чем выбросить какие-либо документы с закрытой информацией в какую угодно мусорную корзину, их необходимо измельчить в бумагорезательной машине.
Информация отделения. Прежде чем выбросить какие-либо документы с информацией отделений компании в общедоступный мусорный контейнер, их необходимо измельчить в бумагорезательной машине.
Открытая информация. Документы с открытой информацией можно выбрасывать в любые мусорные корзины и контейнеры или сдавать на переработку как макулатуру.

Самый простой и дешевый для злоумышленника способ получить нужную ему информацию — непосредственно запросить ее. Каким бы грубым и банальным этот способ ни казался, он неизменно остается главным в арсенале злоумышленников, использующих методы социотехники. Для получения информации с помощью этого способа злоумышленники используют четыре стратегии.

1. Запугивание.
2. Убеждение.
3. Вызов доверия.
4. Помощь.

Защитить пользователей от атак, основанных на описанных персональных подходах, очень сложно. Некоторые пользователи в силу своего характера имеют больше шансов стать жертвами атак, основанных на каком-либо из четырех этих подходов.

Служба поддержки — важный механизм защиты от социотехнических атак, который не стоит недооценивать.
мусорный контейнер